Nicolae Sfetcu

# Beginner's Guide for Cybercrime Investigators

MultiMedia Publishing

# Beginner's Guide for Cybercrime Investigators

Nicolae Sfetcu

Published by MultiMedia Publishing

Copyright 2018 Nicolae Sfetcu

Published by MultiMedia Publishing, https://www.telework.ro/en/publishing/
ISBN: 978-606-033-093-6, DOI: 10.58679/TW15465
Book text available under the Creative Commons Attribution-ShareAlike License

**DISCLAIMER**:

The author and publisher are providing this book and its contents on an “as is” basis and make no representations or warranties of any kind with respect to this book or its contents. The author and publisher disclaim all such representations and warranties for a particular purpose. In addition, the author and publisher do not represent or warrant that the information accessible via this book is accurate, complete or current.

Except as specifically stated in this book, neither the author or publisher, nor any authors, contributors, or other representatives will be liable for damages arising out of or in connection with the use of this book. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory; direct, indirect or consequential damages, including for third parties.

You understand that this book is not intended as a substitute for consultation with a licensed, educational, legal or finance professional. Before you use it in any way, you will consult a licensed professional to ensure that you are doing what’s best for your situation.

This book provides content related to educational topics. As such, use of this book implies your acceptance of this disclaimer.

# Contents

## Contents

Computing systems and storage media ..... 7
Computing devices ..... 7
Peripheral devices ..... 7
External drives for media storage ..... 8
Typology of data stored on specific supports – File systems ..... 9
Program that allows working with ” inactive” space ..... 10
Information that can be obtained from the computing system environment ..... 11
Computer networks ..... 12
Copper wire in computer networks ..... 13
Optical fibers ..... 13
Wireless LAN ..... 14
Internet and Intranet ..... 15
Software and services ..... 17
Client/server architecture ..... 17
Protocols and Standards ..... 18
Internet Services ..... 19
e-Mail ..... 19
HTTP ..... 22
Web address - URL ..... 22
Web browsers ..... 23
Working with web pages ..... 24
Proxy servers ..... 25

Privacy on the Internet ..... 26
FTP ..... 27
Instant Messaging ..... 28
Peer-to-peer networks ..... 29
Vulnerabilities ..... 31
The first attacks on the Internet ..... 31
Cybercrime ..... 31
Typologies of cyber attackers ..... 32
Classification of risks and incidents in cyberworld ..... 34
Classification as a list of terms ..... 35
List of categories ..... 36
Categories of results ..... 36
Empirical lists ..... 37
Events, attacks and incidents ..... 37
Online security events, actions, and targets ..... 38
Actions ..... 39
Targets ..... 39
Attacks ..... 40
Tools ..... 40
Vulnerabilities ..... 41
Unauthorized results ..... 42
Cybercrime laws ..... 44
The concept of "cybercrime" ..... 44
Investigations ..... 49

Computer forensic investigations ..... 49
Digital evidence ..... 50
Digital sampling during investigations ..... 51
The suspect ..... 53
Witnesses in cybercrime ..... 54
Transporting of samples in laboratory ..... 54
Analysis of samples ..... 54
Preparing team members ..... 55
Computer tools ..... 56
Convention on Cybercrime ..... 57
Preamble ..... 57
Chapter I – Use of terms ..... 59
Chapter II – Measures to be taken at the national level ..... 59
Chapter III – International co-operation ..... 70
Chapter IV – Final provisions ..... 79
Recommendation No. R (95) 13 ..... 85
Appendix to Recommendation No. R (95) 13 ..... 86
I. Search and seizure ..... 86
II. Technical surveillance ..... 87
III. Obligations to co-operate with the investigating authorities ..... 87
IV. Electronic evidence ..... 88
V. Use of encryption ..... 88
VI. Research, statistics and training ..... 88
VII. International co-operation ..... 88

Rules for obtaining digital evidence by police officers ..... 90
Standards in the field of digital forensics ..... 91
Principles in digital evidence ..... 92
Procedures model for the forensic examination ..... 93
Hard disk examination ..... 93
Code of Ethics ..... 95
Sources and references ..... 96
About ..... 98
Nicolae Sfetcu ..... 98
Contact ..... 98
Publishing House ..... 99
MultiMedia Publishing ..... 99

# Computing systems and storage media

## Computing devices

The computer itself is the main source of information for the investigator. In the computer, information is stored on the hard disk. A hard disk drive is a device that can record magnetic data, consisting of one or more rigid discs, read / write heads and mechanical mechanisms protected by a metal casing, hermetically sealed. The storage capacity of a hard disk is normal nowadays tens or hundreds of gigabytes. A computer may have one or more hard disks of different types and capacities.

Laptop computers are computers designed to be easily moved. Because of performance reached, some users may be used as permanent workstation.

Types of portable computers are:

- transportable / smartphone
- laptop
- ultra-light
- hand (also called Pocket PCs, Palm or PDAs , personal digital assistants)

Even if they are not used permanently, portable computers are an important source of information, because they can be used for storing data, confidential as possible, to be carried off locations where security is ensured.

Lately due to technical possibilities to miniaturize computing devices, they have been integrated into small portable equipments. The best example of this is the mobile phone which has got features mini-computer. Besides the recent calls log, a modern phone can contain lists of addresses, schedules meetings, documents and notes etc. with even higher capacities than PCs a few years ago.

### Peripheral devices

- the *keyboard* is not intended for information storage, being only an input device. However, there are some devices that can attach keyboards and can record keystroke sequences users. Although very little spread, these devices are very easily available.
- *monitors* are capable of storing information. in the past, due to technical limitations could cause images or text that remained on the screen for a long

time, the impressions produced on CRT phosphor. Modern monitors do not show this effect.

- *printers* can be sources of important information. For example, laser printers allow revealing image type prints last. This technique should be used before disconnecting the printer from the mains electricity supply, which requires the presence of an expert at search. Some laser printers have a disk buffer that stores information to be printed. The capacity of such a disc is from 2 to 10 Mb. Data stored on these disks can be objectified according to a relatively simple procedure. For older models of printers that use cartridges Band (ribbon) can be reconstructed by examining the print ribbon. Assimilation analysis method is printed ribbon typewriter.

## External drives for media storage

External drives for media storage are:

**CD- ROM** (acronym for Compact Disc -Read Only Memory) are data storage devices on optical disks using compact – disc technology. The data is read with a laser -based system and not on magnetic media used for other data storage methods. Some CD- ROM drives (CD recorders) can be used for recording data on optical media.

*CD – Compact Disc*

**Diskettes**. Floppy disks with 3.5 inches in size. Floppy disk is a data storage medium selective for the user. Saving data on disk is performed by users for various reasons, such as creating backups of important files recording data that the user wishes to store the computer company, copying files to transfer to another computer, etc.

*Floppy Disks*

**Backup disks**. Information from backups created to avoid loss of information in case of a power outage are an important source for investigators. Same time with the lifting of backup discs must be recorded as much information on how are achieved the backups, especially the types of equipment, software and procedures used. Safety information is usually stored in large-capacity optical discs, for this purpose, such as the type Zip or Jazz disks, Iomega products, but may exist on any storage medium. Lately became very popular flash memories, very small in size, with large enough capacity.

*USB drives (Flash drives)*

**Optical discs** (most popular being the CDs) are high capacity storage media for digital data. The capacity of these discs is 650 Mb (CDs) to 4 GB (DVDs). Optical discs can be either normal (read only without the possibility of data recording), recordable (possible reading and writing data to disk without deleting data) , or with the possibility of rewriting (it is possible to read, writing and erasing data on the disc).

**Removable hard drives** are also information storage mediums. They have capabilities similar to the fixed hard drives, and are generally used to transfer large files.

*Removable hard disks*

# Typology of data stored on specific supports – File systems

The primary function of the information systems is to store and process data. Data processed and stored by the computer systems can be classified into four categories: active data, archived data, safety saved data, and residual data.

**Active data**: information available and accessible to users. They are presented in different forms, such as documents created by word processors, electronic calendars, mailing lists, files, graphics, audio files, etc. .

A special feature is that for computer data the copy is absolutely identical with the original (the copy does not change anything). Recording active data can be done with special software called file management, execution of specific commands, or operating systems.

**Archived data** are information that are no longer commonly used, and are stored separately, to free disk space. Archived data also include duplicate files. Duplicate files are automatically created as computer files in case of technical problems (such as system crashes, power supply interruption , etc.), with data recovery role. They have specific file endings, and are usually stored in different locations of the original files. Their importance lies in creating multiple copies of documents, copies that user can erase, and whose existence most often is not aware. By comparing the original with duplicate copy, can be made observations on the changes between different versions of the document.

**Safety saved data security** (or **backup data**) is information copied on removable media with the aim of making their data available to users for a power system intervention. How often backups it depends both on type of systems (network connected computer, or computer network ) and user procedures.

For networks, the typical practice is to create a full backup once a week, usually on Fridays, and daily implementation of additional copies aiming at saving the data modified that day, in these cases, usually copying only the information which is on network server, which is not the computers (terminals ) users. At the end of the month is backed the safety copy, which is stored separately and kept for a period of time ranging from several weeks to several months. In practical environments the support where is made the copy is to be used again after a month period.

For computers that are not connected to the network , without a proper backup system, their owners usually copy the files to which they attach more importance, on a storage media such as hard disks removable, recordable CDs, flash drives , etc.

Using information from the storage media for backup storage is useful due to the information kept for a long time. But, due to the lack of organization of the data on these environments, and that usually safety saved files are compressed for the economy of space, it makes it more difficult for investigation.

**Residual data** is information that apparently were removed from the system but persist in specific forms and can be recovered. Such residual data are deleted files that are still on the disk, temporary files, file exchange, data in the active space, the data buffer and clipboard.

If normal file deletion, data is not removed from the disk, but the computer marks the portion where file was placed as free and can thus be rewritten. If the override does not take place (where deletion was recent, or if there is enough free disk space, and there were no operation of routine system maintenance, such as defragmenting or optimizing), the file, or portions of it, were still on the disk, and can be recovered. For recovery are using special programs. In fact, data becomes unrecoverable on the disk space only after the data have been overwritten 7 times. Special programs can do this operation (overwriting 7 times) to permanently delete some data.

**Temporary files** are files created by the operating system or another program to be used during the session. In many cases, temporary files are not deleted from the disk, and so can be recovered information contained in them.

**Files exchange** (or **swap files**) are hidden files created by the operating system to be used for the preservation of portions of program and data files that do not fit in memory. Exchange files are a form of virtual memory. The information from exchange files can be analyzed with the help of special programs.

**"Inactive" area** (*slack space*) is the space located in a physical unit of data storage on disk (cluster) that is not covered by the portion of the file occupying that unit. Because DOS operating system does not allow to store more than one file in a storage unit, the difference between the current file size and the size of the storage space is considered "inactive", unused. This space can contain information that can be recovered using specific programs. Also this space, as considered damaged drives, can be used by advanced users of information systems to conceal information.

## Program that allows working with " inactive" space

**Buffer** is a memory area reserved for use as temporary storage, where there are temporarily stored data waiting to be transferred from one location to another . Data in the buffer can be retrieved with the help of special programs.

**Clipboard** is a portion of memory, having special character, maintained by the operating systems based on windowed mode (such as Windows). The clipboard is storing data being transferred from one

# Information that can be obtained from the computing system environment

Data files are not the only opportunities revealing information from computing systems. The category of data about the computing system includes recording data auditing, computer activity log, access control list, and other information that can not be printed.

Audit records are a means of tracking all activities affecting some data from the moment of their creation to disposal of the system. They are used by most management programs of computer networks. These records and computer log can provide information about who and when accessed the system, where and for how long, and the operations he made (changes, copying, deleting, etc.)

In addition to the audit records, a large number of companies have special software installed to monitor the use by an employee ‘s own information systems. These programs can provide information about the programs accessed, files used, emails sent and received, websites visited, etc.

Access control list (ACL) is associated with a file list that contains the names of users and groups that have permission to access and modify the file. The user access to those files depends on the employee’s duties or position in the company.

The information that can not be printed are also important sources for investigators. Such information are as follow: date and time attached to each file, information about the creation, access and modification of files (provided, for example, by the text editors), comments and notes not intended for printing, etc.

# Computer networks

There are few computer users who have never used a network. Whether to send a message or to find certain information, increasingly more people are using networks. Both for people, as well as for business, currently being connected to a network is to be able to communicate.

Computers can perform independent almost anything, but it is more effective if available resources are shared. When it is desired that all people in an office to be able to print the documents they drafted, each person can buy a printer. It is a solution, but certainly not the happiest. It's much easier and cheaper to buy one printer that is attached to a single computer and are shared by all others as would be connected to their computer.

It can be said that the main purpose of computer networks is to share resources. These resources are very diverse, among them are modems, printers, storage space for files, and information such as that contained in the database. From this point of view, the computers on a network are divided into **servers** (that serves resources), and customers who use them.

A network is more than two computers connected. It is the equipment, software and the people who created them. Principles of networks, however, are simple enough. Networks are classified primarily by geographical area which can be from a few meters to thousands of kilometers.

Most commonly encountered type of network is in offices or universities, called **Local Area Network** (**LAN**). This may include computers of a department or an entire company or institution. Common area that have such a network is hundreds of square meters.

To connect each headquarters of a company or institution is required to cover much greater distances. Larger networks, which realizes the connection of equipment at great distances are called **MAN** or **WAN**, ie **Metropolitan Area Network** or **Wide Area Networks**.

The technology used for computer networks somewhat resembles that used for phone. Developments in technology will most likely that in the near future the two technologies converge. Theoretically, phones could be connected directly with each other, but in practice this never happens, because it would be impossible. Instead there must be a connection cable with every other subscriber, there is a central one, which has encapsulated functionality to link any of the two (or more) of its users.

This happens for computers too. There are devices that are designed as centrals, coordinating groups of computers and are generally classified depending on the functionality they offer. Among these devices are routers, switches, access points and hubs.

# Copper wire in computer networks

Copper wire is currently the most used medium for connecting computers and network equipment. Among its advantages are primarily low price and high enough speed that can provide data transmission. In addition, the material is flexible enough to be mounted in the walls and drawn by any office.

Over the last few decades have used several types of cable. In the past it was coaxial cable used (very similar to the TV antenna), but lately has become the de facto standard twisted pair cable – UTP ( Unshielded Twisted Pairs ). Networks that use this type of cable has a star-type architecture because all computers are connected to a single device called hub or switch.

Interception of communications through copper cables do not present particular difficulties for professionals, based on the same principles with fixed telephony, but requiring acces to the physical cable. This last fact makes the interception quite rare because copper wire is generally used in offices where access is easily controlled.

# Optical fibers

Fiber optics is a fairly recent technology and leads to much higher capacities for transmitting computer data, being generally used between important nodes in the network or between networks.

While still relatively expensive and difficult to handle and connected, optical fiber is used for connecting LANs inside but found its perfect applicability as part of the infrastructure service providers where the performance and security requirements are higher than the pricing.

An optical fiber connection sections may have up to 4 km, which is another advantage over copper wires that are not covered more than a few hundred meters. UTP and FTP cables have coverage distance up to 100 meters distance to the guaranteed parameters of the network using this type of connection. It is used over longer distances, but there is no guarantee for optimal functioning. Also, the connection parameters can be dramatically perturbed by the "noise" that perceives cable as an antenna. You can use 75-ohm coaxial shielded cables, but in this case meet the same limitations attenuation data over the wire and cable noise may levy.

The optical fiber is based on a "wired" thinner than hair, made of a very pure glass. The data is transmitted in the form of pulses of light (beams of light) which is reflected by the inner walls, therefore goes to the other end.

The technology described above has an unexpected advantage. The entire length of the optical fiber cannot be intercepted, because it emits electromagnetic radiation (electric

current is not running through it, but the light) and may be cut (if the fiber is broken, communication is interrupted in its entirety). This makes it ideal for networks (or network segments) where the confidentiality of transfer is essential. Communication is interrupted during sectioning, but can be resumed as soon as the fiber rupture remedy, even using an adapter that can capture traffic over fiber.

# Wireless LAN

Wireless LAN, also known under the names of WLAN, 802.11 or WiFi, although the most recent connection method in recent years has seen an unprecedented rise in popularity.

This popularity is due even to its main characteristics: lack of cables. Computers connect on the network without the need for cables or connectors. It's a dream come true for those who use mobile PCs (laptops and PDAs) and obtain total freedom of movement within the area covered by the wireless network.

Consider the usual firm, which has the principal office at the 8th floor meeting room on the 2nd floor of an office building.

Wireless network equipment has the main component that is called an Access Point. He is a relay that sends and receives radio waves to and from devices in its range.

In the example above we considered the network are two access points. One on the 8th floor of the building principal office and the other in the meeting room on the 2nd floor. Director can go to meetings taking with him the laptop and although it is not in his office can ask information to secretary or email to inquire for the latest news, all without having to connect any cables.

There is a reverse of the medal itself for wireless networks. Besides the easiest use and the most flexibility, a wireless network is also the most exposed in terms of vulnerability to unauthorized interception.

At the physical level, anyone can access a wireless network. There is no need to cut cables because the data propagation medium is air. They can pass through windows, as well as can pass through thin walls of ordinary offices. Fortunately, it is not generally enough to have access to the physical layer to achieve the effective network access, as communications equipment manufacturers have developed ways of data encryption that make them inaccessible to intruders. Wireless network security is a very bright moot point, because of the reasons unknowingly of users or unprofessionalism of directors, or to allow easy connection, these protective features are not always enabled.

The future is probably a combination of the above technologies, which will also add features coming from the mobile world.

# Internet and Intranet

Computers are connected in local area, metropolitan or wide area networks. In turn, the networks are linked together in what is called the **Internet**.

The Internet is a global network of computers. Any computer connected to the Internet can communicate with any other computer connected to the Internet. It can make analogy with road network that allows a car to starting a village to reach any other village. There are smaller or larger streets, and the route used is not necessarily straightforward.

The Internet is a decentralized network, meaning that there is no institution or a state that ail his own or govern the operation. Financial and logistics support is carried out by companies whose accesses and management is overseen by a committee called *ICANN* (*Internet Corporation For Assigned Names and Numbers*).

Because everyone in the world can connect to the Internet without restrictions, it is considered as public. Like any entity open to the public, Internet presence involves a considerable risk, both for people and especially for companies. Being an open space, the Internet allows individuals or organizations to cause malicious damage other members more than any other network.

Given that information has become very valuable, fraud temptations for containing systems became increasingly larger. Given that reason either financial interests, or simply entertainment, crime found a good place in computer networks.

To enable companies to protect themselves from threats from the Internet, and also to be able to use the advantages that make it so popular, it is using an architecture that is called **Intranet**. The intranet is a private network (as opposed to Internet which is public) within a company or institution. Intranet computers inside are not accessible from the outside, but can access both internal resources and resources from Internet servers. This is possible using a device called **firewall**. It is basically a filter which allows only connections in a single direction inside to the outside. A pretty good analogy foe firewall is a private PBX, found in most companies with more than two offices. A firewall does not close completely access from the outside, only if programmed to do so; firewall connections are bidirectional. A firewall does not block, currently, only those unauthorized connections from the outside, leaving the intranet users to access resources from both the Intranet and the Internet. Users outside the Intranet can access only that information that the firewall allows access and is configured to provide them.

Like phones, computers use numbers to be identified. These are organized into four groups of numbers separated by the character ". "(Point), called **IP addresses**. Computers in a network are assigned consecutive groups of 256, 128, 64, 32, 16, 8 or 4 addresses based on the number of devices to be connected. A special type of IP address is the **private addresses**. These are similar numbers inside the PBX I mentioned above.

Private addresses are easily recognized because they have a standard form, as 10.xxx.xxx.xxx, 172.16.xxx.xxx, ie 192.168.xx These addresses are used only to computers intranets.

The connection between two networks is done using a **router**. It has one connection for each network to which it belongs. In general, the router may be a dedicated equipment, itself an ordinary PC can serve this role.

The router acts as a dispatcher, which decides which network is intended for information it receives, often with the added role of firewall. It is the most widespread of Internet equipment, after PC, the point of entry and output of information between networks. It is a common fact that between two computers on the Internet to be used several routers (may be even a few tens) in transit.

*Information received by the PC user from the partner server throughput multiple routers*

Because of the important role it has, the router is the most delicate networks equipment. Being the equipment through which transit so much information, his compromise is equivalent to the access, usually unauthorized, to all this information. When controlling access to the router that connects to the router through which a companz connects to Internet, not only that zou have access to all the messages that the company submit its partners, but also get an open door to the inside protected network.

*When a person compromises a network router, is likely to get control over other resources*

# Software and services

## Client/server architecture

Internet and most networks use the principle of client/server. Servers across the globe provide certain types of services, and clients (PCs, laptops or mobile) connects them to access the information.

The main reasons for using so wide of this architecture are:

- storing information in one place, where it can be easily redistributed to customers;
- dedication of computing resources (servers) for specific tasks such as for example email - where safety is involved moving information from one point to another.

Customers (ie those who work with computers as a network client) can have a huge variety and can be off and on without affecting the proper functioning of the network.

What should be noted first of all that the vast majority of Internet services is that there are:

- a program (software) client on the one hand;
- a server program on the other side;
- connections between client and server;
- connections between multiple servers;
- direct connections between clients.

The transfer of files from the server to client is called *downloading*, and the reverse is called *uploading*.

In all these cases, the relevant from the point of view of security is the answer to the following questions:

- who "talks"?
- with whom?
- which way?
- what information changes?

# Protocols and Standards

The main difficulty that occurs when so many computers are interconnected is to find a common language to exchange information. This difficulty is resolved by adopting global *standards*. In the Internet world, as in other communities, defining these standards is done in a collaborative manner. Basic Internet standards are described in documents called RFCs (*Request for Comments*). There are people who are responsible for maintaining this documents, anyone is welcome to complete and comment.

These documents are to define the *protocols* used on the Internet. A protocol is a language (data format) that two computers use to send and receive information.

There are a variety of protocols from which to choose. Each has advantages and disadvantages; for example, some are easier than others, some are more secure, while the other is faster.

The place where you can find very comprehensive information about protocols is http://www.ietf.org/rfc.html. Here are the RFC documents for each Internet standard. Each of these documents has associated a number 3 or 4 digits. For example, RFC822 treats aspects of the format in which are shared emails.

To understand how the internet works, you must understand how computers communicate with each client and server. There are two communication types that are important: *connectionless* mode and *connected* mode. This is based on the transfer of **packet** data.

- **TCP** (*Transmission Control Protocol*) is the connected mode of communication. Customer is temporarily connected to a server, after negotiating a specific channel. Communication is made via packet data, but there is an order to them, their continuity being ensured. This mode is similar to the phone, meaning that in order to speak it establishes a temporary connection;

- **UDP** (*User Datagram Protocol*) is the connectionless mode of communication. It is similar to the postal system, meaning that packets of information (letters) are generally sent without acknowledgment, in the hope that they will arrive without a real connection between sender and receiver.

Most relevant protocols for the topic are based on TCP, the mode of transmission of information based on the connection.

Every computer and therefore each server has an IP address. How a computer can define multiple services, there must be a way to identify these services. It uses the concept of **port**, that is a number that identifies the service to be accessed. To best understand the reason why there is this concept, the easier it is to think of an address: to find a person is not enough to know the address of the building where they work - ie the IP address for the computer, but the number of office or room - that port.

In short, the port number indicates to the server the service you wish to access. For example, 80 is the port number for **HTTP** (*HyperText Transport Protocol*), used to transfer pages on the Web sites.

IP addresses are numerical in nature, to be easily used by computers. But people retain hardly the random numbers, and for this reason was designed a service, called **DNS**. DNS stands for *Domain Name Service,* and it is for the network which is agenda for the phone numbers of friends, the difference being the scale of operations performed. A DNS server contains the correspondence between name servers and thus their IP address, as phonebook contains correspondence between the names and their phone numbers.

Computers are organized into domains, nested each other. A server or a computer can belong to a domain even though it is not even on the same continent with the other.

To uniquely identify a computer, it is writing the domains separated by points, starting from the lower unit.

Similar to a regular mailing address, the e-mail adress is using the form user@domain-name.com, eg johndoe@gmail.com.

# Internet Services

## e-Mail

E-mail is probably the service that has contributed most to the increase in popularity of the Internet so great, still one of the main reasons that people connect to this network.

The key to success lies right in its features: it is fast, very cheap and is an excellent way of communicating with others, because a message can contain any text, images, music or videos. In addition, while an ordinary letter needs days or weeks it should be received, a message would be enough usually a few seconds to reach the other side of the planet.

In terms of privacy, however, things are not so good. Although generally the symbol used to represent the service is a sealed envelope, in reality things are not so at all. A more appropriate symbol for e-mail would be the postcards.

Although a card cannot be read by anyone, it is enough to know that the postman can consult before delivery to realize that you should not write your PIN credit card site or a declaration of love secret behind thereof. Similarly, email messages are transferred into network using clear text, which, combined with the slight possibility to intercept them, makes them very vulnerable.

The most common method to protect the e-mail is to encrypt. Two technologies are used in general to do this: *PGP* (*Pretty Good Privacy*) and *PEM* (*Privacy Enhanced Mail*). Both allow

both message confidentiality by encrypting content and verification of the origin using digital signatures.

Encrypt messages, although percentage increased in recent years, remains very little used, making the mail to be considered an unreliable communication medium. Despite this, e-mail incidents are quite rare.

To send and receive electronic messages there are used multiple protocols: *SMTP* (*Simple Mail Transfer Protocol*) to transfer messages from the sender to the server, and between servers, ie *POP3* (*Post Office Protocol*) for receiving mail. Another protocol is used for email is *IMAP* (*Internet Message Access Protocol*), an improved version of POP3.

In general, the network service provider - *ISP* (*Internet Service Provider*) is responsible for creating mailboxes. They have associated one or more e-mail. A mailbox is not only a file server, e-mail, where are collected the addresses associated inbox. When the client connects to the server, is transferring messages from these files on your own computer.

The figure below describes the process that takes place to send a message from George Smith of the Ministry of Transport by John Doe, working at the London branch of IBM:

Steps that are performed are:

1. George compose the message in his mail program (client application). Fill in the *recipient* field (*To* :) the e-mail address of John.

In this program is configured the mail server name that contains his post box (corresponding to the address george@mt.gov).

2. When you press *Send* button of the program, it establishes a connection between his computer and port 25, the SMTP protocol corresponding of the server, connection used to send to this the message contents.

3. Mail server receives the message and one of its programs (server application) examines information about the recipient. From address john_doe@uk.ibm.com cut the server name, ie uk.ibm.com. Using DNS service, find its IP address.

4. Mail server of the Ministry of Transport establishes a direct connection with uk.ibm.com server whose IP address determined in previously step, sending through the established channel the message for Joe.

5. UK server gets the message, validates recipient, verifying that john doe is really a system user, and stores the message in the electronic mailbox of John.

6. When John PC connects to the Internet and John request receiving mail, client program connects to the server using POP3 protocol (port 110) or IMAP (port 143). With the connection established, from the server is transferred all messages from the last request.

7. Client program of John processes received data and displays them on the screen.

**Spam**

Spamming is the act of sending large numbers of unsolicited electronic messages (usually of a commercial nature). Although there are several methods, the most used is based on e-mail. Spam in the form of text messages may also target mobile phones.

Spam involves sending identical or nearly identical unsolicited messages to thousands or millions of recipients. Unsolicited message means that the recipient has not granted permission to receive that email. Message sent wholesale (bulk) means that the message is part of a larger collection of messages, all having about the same content. Their addresses are collected from focus groups of web pages, obtained from databases or simply guessing, using the common names and domains. To be spam, a message must be sent unsolicited and wholesale. Unsolicited messages are normal messages (such as achieving a first contact for sales, job search, etc..). Similarly, messages sent wholesale (bulk) are normal messages (electronic newsletters, mailing lists, etc..). Only the combination of unsolicited and sent in bulk is spam.

Increasingly, many states consider it a practical reference itself unsupported.

Statistics have shown that the most annoying phenomenon from the point of view of people using the Internet is spam, that one of two e-mail is unsolicited and more than two-thirds of the deals are illegal.

The main products that are advertised in these messages are pornographic websites, software, pharmaceuticals, credit card accounts. Also spam is promoting things like pyramid schemes and false business proposals, the most famous being "Nigerian fraud" ("Sir, I need your money to be able to take out $ 2 million from a bank in Nigeria. Instead of aid, you will receive 40% of the money ").

Spam is considered unacceptable behavior by both service providers losing money by advertisements processing others and by users that messages are very irritating, most times offensive, moreover it causing losses time for reading them. Because spam is sent to e-mail without discrimination, is possible that advertisements for pornographic sites appear on the computer at work, or worse, on a child's computer.

The act of sending unsolicited is a violation of policy to use the services of most of the ISPs and may lead to suspension of involved access. Spammers endeavor to hide from where the message was sent. They do this by simulating e-mail, so that the message appears to come from the latter. Although it is not possible to completely hide the origin of the message since the server's IP address is recorded originator server, catching the perpetrator is very difficult. Commonly used names, addresses and phone numbers to create false inbox messages to different Internet providers, in many cases these accounts are created using

counterfeit or stolen credit card numbers. This allows them to move quickly from one account to another when they are discovered and their rights to send suspended.

## HTTP

*Hyper Text Transport Protocol* (*HTTP*) is the core of traffic on the *World Wide Web* (or *WWW*) on the Internet or private networks, and is basically a very simple protocol. It establishes a connection, and it asks for a document, by sending sometimes a set of parameters.

HTTP was originally created to serve the better organization of documents in the academic world. The initial basic concept when it was projected was, as the name suggests, one of *hypertext*. This is a representation of information where can be created connections between objects (text, images, videos). When an object is selected, you can see the objects related to it. For example, reading a document about classical music, a click with the mouse on the *Concerto for Harpsichord and Orchestra*, makes the screen to display more information on this creation, and clicking the name of Mozart may display a picture of the composer . Another click can download an audio file containing the concert.

This concept allows very good organization of information dispersed by forming links between them as a mesh network (*web*). When information is stored on computers around the world, this network becomes *World Wide Web* or *WWW* shortened.

Here it is a description of the components involved in an HTTP transfer:

- *client software*: Usually called the *browser*, the most popular such programs currently being Internet Explorer, Google Chrome, Mozilla and Opera;
- client *computer* that is connected to a network (usually the Internet);
- *server* connected to the same network as the clients that are accessing;
- *applications* on server that implements the HTTP protocol.

## Web address - URL

Generally, the transfer begins with a request that the client makes to the server as a result of a user action such as entering an address or clicking on a link. The addresses are also denominated as **URL**, acronym for *Universal Resource Locator*. These specify the protocol to be used, the server and TCP port, indicating the information that you want to search.

- *http://* - protocol used to transfer information. In this case it is HTTP but, as we shall see below, it may be https://, ftp://, irc :/ / etc. Protocol specification is required in order to establish a common language between computers. If this mechanism should be applied to mobile ie, they would form *Romanian :/ /*

*0745526896* for a conversation that is expected to be in Romanian, respectively *English:/ / 0745526896* or *fax :/ / 0745526896* for other "protocols".

- *www.teleactivities.com* - name of the server to which the connection must be made
- */information-technology/* - the path of the resource you wish to access.

## Web browsers

In terms of investigations, it should be noted that the accessed links are generally temporarily stored in the client programs. This feature called **History** - history of navigated pages, and can be a very useful tool for research pages that were accessed by a possible suspect.

An interesting aspect is that the addresses of *History* also contain other information. The URL parameter can appear to help the server to compose appropriate response.

It is noted that the search terms are added to the search URL, separated by the symbol "?" and containing the parameters in the form name=value. They generally should not be entered manually, are generated by the browser in response to a user request.

If in the PC of a suspect appears an address that you are interested in it, it can be concluded the him probably sought and obtained information about the searched terms.

Browsers also offer other facilities that can be used to investigate a suspect's actions. These are the *list of bookmarks*, *temporary storage of data last accessed* (*cache*) and *cookies*.

The list of bookmarks, generally referred to *Favorites* or *Bookmarks*, give to the users the possibility to track interesting pages they visit. This list is personal and is easily accessible when the browser is opened.

Browsers are optimized to reduce network traffic that is not required, meaning that files are transferred each time they are displayed. Instead they are stored temporarily (for a few hours, days or weeks) on the local disk. When the user wants to display a page, the browser first checks whether text, images or files not already accessed it. If this has happened, their content has been transferred from the server, thereby dramatically browsing speed and comfort.

This process is called *caching*, in terms of investigations is very important because many samples can be gathered by examining the contents of files it contains. The location of these files depends on the operating system and browser. Until now, all browsers keep unencrypted contents of these files, making easier to examine.

*Cookies* are small text files that are on your local disk. They contain information that assists the browser and the web server to display a user customized pages for sites that offer

dynamic content. May also contain your user name or password for a page. The contents of these files is defined by the creators of websites and they are usually stored unencrypted, as well as cache.

### Browser cookies

Provided as a facility built into many browsers, cookies can monitor and chronicle an individual's visit to the web sites, what they look at and how long they spend in different areas. Also, they can find out if the visitors have been to the respective site before.

By themselves, cookies will not even reveal the name and address of the visitors. The real power from cookies is when they are linked to other information. Typically, this is when registration forms are used to gain access to a particular web site.

In some situations, cookies can act as a password, or can be used to store ongoing orders – a sort of virtual shopping basket that store items selected for purchase, even if they are amassed during several web site visits – and are activated as far as the company is concerned only when the visitor presses the buy button.

Cookies can also to present an individual visitor with personalized preferences based on the topics it shows as having been of interest before.

Cookies are not just for web tracking but for added value. In the case of regularly visits, the cookies become part of an intelligent learning process based on what the visitor looked at before.

But the cookies were presented generally as "web spy". It is true that information gained by cookies can be swapped or sold to a third party company that centralizes it attaches it to other information and a whole chunk of an Internet user's life could be available to anyone who pays for it.

## Working with web pages

### Choosing your favorite web pages

To have direct access to web pages that are of particular importance, without having to navigate through the pages of their websites, it is advisable to use the option "Bookmarks" in your browser. Thus, when browsing the Internet and discover an interesting page, you can add to the "Favorites". Arrange of addresses can be done anytime with the option "Organize Favorites" (or "Show All Bookmarks").

### Keeping track of visited web pages

When you visit a site browsing the Internet, address is automatically saved in "History" in the browser.

Here can be found a history of all sites visited in the last three weeks, in alphabetical order or date order. For the current week, day record is held.

The menu features address from viewing by date, alphabetically or by number of hits. Also, you can search the visited websites by keywords.

### Saving web pages

Saving web pages allow their retention on disk for longer, so they can be accessed even without Internet connection. Saving can be done in the following ways:

- Web Page, complete (full website): The page is fully saved with original formatting of the page.
- Web Archive, single file (the archive page, in a single file): Web page is saved in an archive file completely. This method is not always available so if you want a full copy of the original page, it is recommended to use the first way.
- Web Page, HTML only (web only content html): This mode saves the information as a text only page content, the original editing, but not other files (graphics, photos, sounds). The file has this way a small size and allows a better view of the text because it is the preserved original placement on the page.
- Text File (text file): page content is saved in plain text format, thus losing the original formatting. The file takes up very little space and is used mainly for saving pages containing mostly text without special formatting.

## Proxy servers

There are increasingly many companies which, along with the use of a *firewall* equipment, use for HTTP *proxy servers*. They are designed to be intermediate between the client and the web server, making connections on their behalf. Usually they contain a powerful caching *mechanism*.

The good part of a proxy server is that it has a history of pages that were accessed using it. That makes it relatively easy to investigate by obtaining evidence when it is available to those who are investigating the case. The downside is that the proxy server logs are not available, for reasons of confidentiality or jurisdiction (may be anywhere in the world), the suspect can not be found, the registration connection appears to have been made by the server.

Consider the example given by the figure above, suppose we want to identify all users who use the site http://www.website.com/. The first stage is carried researching the web server log. Here is available the next record:

2004 February 14 03:04:14 [proxy_c.private_company.com 180.196.222.16] "GET / HTTP/1.1"

From this record it can be inferred that at 3 am on February 14, a user with that address 180.196.222.16, meaning a proxy_c.private_company.com, accessed the website. Contacting the company, it says that the address is a proxy server that serves all users.

The next step is for the company to provide proxy log records. Here are seeking proper registration of the web server, which has the following form:

2004 February 14 03:04:13 george@client_b "HTTP/1.1 GET http://www.website.com/"

This latest evidence leads to the conclusion that at that time, the user george on the PC called client_b accessed researched website. Statement is sustained ny the company representatives too, who say at that time in the building was only George, the night watchman.

Usually investigation continues on PC client_a, to obtain evidence supporting the History, Cache, Cookies, and Favourites.

## Privacy on the Internet

As the protocols used for e-mail, HTTP uses broadcast of its messages clearly, making it vulnerable to even novices attackers. A simple solution to ensure the privacy of navigation is using an extension protocol called *HTTP Secure* or *HTTPS*. Addresses using this safe protocol for communication can be distinguished easily because they begin with **https://** instead of *http://*.

How HTTPS is more complicated and a major consumer of computing resources, its use is generally limited to the pages where the need for confidentiality is large enough, for example, pages that collect personal information or the management of bank accounts . Also, it is not up to the user to use HTTPS, but the availability of this option on the server to which the user is connected; HTTPS service involves purchasing an SSL digital certificate and its implementation as a service to the service port on the server.

Browsers are controlled entirely by the user and a person who wants to erase the marks on your own PC can do quite easily if it has knowledge.

# FTP

**FTP** stands for *File Transfer Protocol*. His name reveals the purpose for which it was designed: it is used to transfer files over the Internet or generally over the TCP/IP networks.

Its popularity has declined in recent years due to the success that had HTTP, which can also transfer files. But it is rather used as one of the very old protocols has become a "classic" protocol, each operating system having a client or server. In addition, much information gathered over the Internet history is only available on the FTP servers.

Current HTTP *browsers* are capable to use FTP also, so it is very easy for the user to benefit from this protocol.

It can be seen that surfing is like for a file system on a local disk. URLs begin with *ftp://*, its structure being identical to that web addresses.

FTP uses two ports (21, 20) and two connections for communication. A connection is used for interactive transmission of commands and one for data transfer.

Generally at the entry in systems authentication is required using a *username* and a *password*. There are many servers that offer *anonymous* access to their resources without the need for authentication.

The easiest way to gather evidence from a FTP server is to investigate its directory structure and to *download* the files with access rights.

FTP servers have logs that record all connections and transfers made. For example, registration of the transfer of a file containing an illegal copy of the movie *Casablanca*, would have the following form:

Feb 19 23:32:42 ftp proftpd[4652]: connect from 87.17.250.79
Feb 19 23:32:48 ftp proftpd[4652]: ANONYMOUS FTP login as 'anonymous' from 87.17.250.79
Feb 19 23:33:10 ftp proftpd[4652]: 87.17.250.79 /opt/filme/Casablanca-DvX.avi 687094582b
Feb 20 02:17:22 ftp proftpd[4652]: ftp connection to 87.17.250.79 closed

On the client side, the investigations are difficult because not all client applications have logs of transfers. You can check the browsing history, temporary storage on the computer or favorite links on the investigated computer.

# Instant Messaging

Instant Messaging - IM - is the service which it says it will dethrone the future e- mail as the most popular means of communication. It is not a specific protocol , but a concept.

As people began to spend increasingly more time online, connected to the Internet, programmers creatively exploited the opportunity created by this leading communication one step ahead. Instant messaging has "invaded" the Internet in November 1996 when Mirabilis, an Israeli company founded by four programmers, launched ICQ (acronym very similar in pronunciation to I seek you), a free program that anyone can download it and to use it.

The main difference compared to the e- mail is that this type of communication focuses on the immediate sending of the message recipient. The user creates a list of other users with whom he / she wishes to communicate. When a person from the list becomes available, that enter the network, the service alerts the user and allows immediate contact between the two.

The advantages are obvious. Communication is very rapid and is made when two users are both available. The problem of spam disappears, and e- mail formalism imposed by its resemblance to classic mail disappears. Instant messaging can be compared with the phone as real-time communication, where both parties are available.

Companies have noticed the advantages of this type of service and began to implement it widely becoming larger, increasing employee efficiency through faster communication as comparable with e -mail, and arranging online meetings, much less consuming time compared to traditional.

In terms of investigations, IM problems are similar to those of IRC. Although companies that produce programs and coordinate client servers are in small numbers, they do not supervise their messages in transit. Community development is as important as the IRC, instant messaging relying generally on friendly relations and cooperation existing.

Logging messages sent and received is possible for all instant messaging programs, but it can be easily disabled, discovery of evidence relating to messages sent through the service is so uncertain. One advantage is however that contact lists are usually stored locally and is possible to establish a circle of knowledge of the person being investigated.

Regarding confidentiality, IRC and IM applications using mostly unencrypted transmission of messages, making them very vulnerable to interception. However, many users, especially in companies, have realized the need to safe communication, this vulnerability is likely to disappear soon.

# Peer-to-peer networks

Almost overnight, consumers everywhere have adopted an innovative technology that allows them to participate in a broader vision of the Internet. Distributed applications such as *SETI@home* have provided millions of users the opportunity to contribute to processing resources of their computers in order to participate in a common computational effort. True applications peer- to- peer (P2P), represented by Napster, Gnutella and Freenet, have provided an intuitive easy way for users to find and share resources directly with each other, often without the need for a server of a central authority.

In contrast with the Internet philosophy of being a network of interconnected networks, mainly way program applications aiming philosophy was that of client- server philosophy. First used in local area networks, client- server applications could run at the beginning only in homogeneous networks (with compatible computers, and usually from the same manufacturer), without offering any interoperability between applications.

The web has made client-server applications to be accepted very widely, accepting a universal client (web browser) that uses a standard communications protocol. Anyone with a compatible device, from mobile phones to PCs, can use this model.

Newer applications sharing files addressed simple needs and the success of these applications have changed the way people think about using the Internet. Returning to the basic model used to design the Internet, they can interact directly, without using a web server, e-mail or IRC. The network thus seems stronger as users discover a new style, complementary use of computers, which necessarily requires a lot of clients and servers in a default hierarchy.

Currently the most popular P2P application usage is to give and download files. Most common among files in peer -to- peer networks are MP3 files containing various songs and DivX files containing movies. This has led many observers, among which are the vast majority of companies in the music and film industry, to conclude that these networks are very serious threats in terms of income, or even their existence. RIAA and MPAA, representatives of artists and media companies in the United States, have acted immediately to court services companies (software and search mechanisms) file sharing. Napster network was closed after such a process, both groups spending huge sums to determine the imposition of legal restrictions. Strongest manifestation of these efforts to date has been the introduction of a provision in the state of California, which allowed legal copyright holders to access computer systems that were suspected of illegally distributing copyrighted material on one side and stop work peer-to-peer networks, on the other hand. The provision was withdrawn shortly, but it is always possible reintroduction.

As the attacks from the media companies have become more powerful, file-sharing networks seem to adapt in a fast pace, becoming increasingly technologically difficult to stop.

This meant that the targets will be no more the networks themselves, because there are virtually no technical means to be stopped, but their users. Companies are pursuing sharing service users, trying to determine their identity and, if successful, accusing them individually for illegal possession of copyrighted material.

This method has not too much chances to resist in time, because users answer most likely will be that they use encrypted sharing systems that do not allow detection of transferring files. Another trend to avoid the media companies is to use 'ad-hoc' wireless networks, in which each device is connected directly to the neighborhood.

The evolution of the conflict between the entertainment industry, which sees its financial interests threatened, and users who want to get free latest movies and favorite artists songs, is worth watching because none of the parties has not said the last word.

# Vulnerabilities

## The first attacks on the Internet

November 2, 1988 is an important day for the Internet. On that day a graduate of Cornell University in the United States, Robert Morris Jr., executed a worm type program, the first program that has affected in a very serious Internet. In seconds, thousands of computers across the United States have been out of service by the unusual program. Hundreds of networks of research institutes, universities, and of the few companies that were connected to the Internet at that time were affected.

Within a few hours was formed a volunteer group to resolve this situation as quickly as possible. Members of the group called "Virus Net" communicate with their phone and the non-affected segments of the network. After a failed effort to identify cause of the problem, they isolate the virus and find a weakness in the code. This discovery made the spread of the virus to be stopped in a record time of 24 hours after onset.

The way the program called *worm* as it propagates through the network and infected so many computers, is very simple. After infecting a computer, the program create two copies of itself in memory, whose purpose was to look for other computers that may be infected. The two copies are created every turn two copies of the virus. A simple calculation shows that for the 16th "generation" of computers there were more than 65.000 copies of the program on the infected system, and other 65.000 for other computers investigated to see if they were infected.

Because the program was not stopping, he arrived in a very short time to consume computer resources, that was no longer able to respond to legitimate commands of users. Although the problem can be solved by a simple reboot of the computer, it was very likely that he will very soon be reinfected by other systems that were running copies of the virus.

Although it was not catastrophic, the Internet was made up of very few computers at the time (a few tens of thousands, to hundreds of millions that are now), so this incident has put a serious warning regarding security systems in general and networks in particular.

Morris virus has revealed the vulnerability of the Internet and made it aware of the need to secure it, having the same effect on the computer world as the effect of the first hijacking a passenger plane in 1960, within the world of aviation.

## Cybercrime

In the real world there are people who enter the homes and steal everything they find valuable. In the virtual world there are individuals who penetrate computer systems and "steal" all your valuable data. Just as in the real world, there are uninvited guests and people feel happy when they steal or destroy someone else's property, the computer world

could not be deprived of this unfortunate phenomenon. It is truly detestable the perfidy of these attacks. For if it can be onserved immediately the apparent lack of box jewelry, penetration of an accounting server can be detected after a few months when all clients have given up the company services because of the stolen data came to competition and have helped it to make best deals.

Stories about *crackers* and dangerous viruses delight the computer security books and articles. Maybe this is why the greatest danger in ensuring that security is often overlooked. Because most threats do not come from outside but from within.

The notion of *insider* is somewhat difficult to define. For example, members of each department is considered as being inside, people from other departments are regarded as *outsiders*. In terms of security, an insider is someone who is familiar with the procedures and operations of the organization, has friends in the group, while having access to resources and systems offered by this organization.

What makes the inside people even more dangerous is that they are difficult to detect. A stranger is easily noticed when trying to pass one of the barriers between the organization and the outside world, which the member of organization does not need to do.

Computer systems are generally protected from unauthorized access. There are several authentication mechanisms, and then permit of authorized users, but the most common is based on *username* and *password*. A user receives a user name and password that he uses when he wants to access a service or a computer.

Pair *username* / *password* are for computer systems the role is played by the lock in terms of protecting a room from the entry of strangers. The lock is considered a secure means of protection, but in reality there are persons able to open it, for it is not a problem when they want to access the room. The same is unfortunately true for the world of computers.

A special issue on cybercrime is the perpetrators of these types of crimes. The problem of achieving a "sketch" of those who violate law by computer offenses is very current criminological research worldwide. However the authors profiling may be subject to the influence of existing stereotypes in the media. Unanimity of authors consider that offenses committed through computer systems fall into such "white collar crime". A "classic" profile of perpetrators of these crimes can be summarized as follows: male aged between 15 and 45, having a good social status, no criminal record, intelligent and motivated. In many cases , the author is an employee of the company even attacked, or know the functioning of the attacked system.

## Typologies of cyber attackers

There have been numerous attempts to achieve a typology of perpetrators, their classification categories ranging from two to no more than 26. Criteria for delineation of these types are mainly two: the motivations of authors and their legal consequences. The

second criterion makes a distinction between actions that are aimed at causing damage or an undue advantage, and justified the actions of curiosity, or explained by educational reasons. This distinction would legitimize such actions of "hacking", which is unacceptable.

Returning to the first criterion for distinguishing, the authors have defined several reasons. Thus, *Direction de Surveillance de Territoire* from France proposed distinction between playful threats (hackers, etc.), the greedy (financial gain, etc.), and strategic (intelligence, and so on). Three American authors suggest a more complex analysis based on the determinants of criminal conduct, involving motivational elements (having personal characteristics - for economic, ideological, self-centered or psychotic), elements of opportunity (ie environmental features - access to criminal groups, social rewards, different ethics, trust group), means and methods.

John D. Howard proposes the following six categories of authors:

- *hackers* - people, especially young people, entering the systems of reasons mostly related to intellectual challenge, or achieve and maintain a certain status in the community of friends;
- *spies* - people who penetrate computer systems to obtain information enabling political gains;
- *terrorists* - people who get into computer systems in order to produce fear for political purposes;
- *attackers for economic purposes* - penetrate the computer systems of competition, in order to obtain financial gain;
- *professional criminals* - enter the computer systems of businesses to obtain financial gain, for personal interest;
- *vandals* - people who penetrate computer systems in order to cause damage.

**Classification of cyber attackers according to their skills and objectives**

Another presentation identifies five categories of intruders, each with different skills, levels of knowledge, especially with different objectives. All these categories can come from both outside and inside the company.

- The **novice** is usually a lone rookie. No computer experience or how to break into systems from outside. The novice works alone and has no outside help, being often an experimenter who commit illegal acts. It's pretty easy to spot because it is not able to cover his tracks; what is hard is it to be considered a threat. Results of his "work" can usually be found in several locations:
    - files with passwords;

- user configuration files;
- system configuration files.

The best way to fight is to educate novice users, because novices take advantage of deficiencies in the administration of passwords. Almost 80% of unauthorized entry systems happens this way.

- **Disciple** is that novice progressing beyond the initial stages, generally using IRC, exchanging messages with those who are similar. Not only greatly improves their knowledge, but it is part of a network. More advanced members are happy to share their experience and novices become disciples. They learn to better cover their tracks and to enter or leave the system without attracting attention. And although do not know yet modalities of security systems, but have learned how to do so as not to leave marks. "Disciples" most times get through password protection systems and know something about other security systems, which makes them a little harder to catch.

- The **visitor** is probably the most "innocent" of the attackers. These people are simply curious. It is seldom that they compromise systems unless they meet a serious opportunity. If a visitor will find an obstacle, the more often will retreat, seeking another system where access is easier. An exception to this rule, very rare, where the visitor noticed an interesting thing and is willing to spend some time longer for him to study.

- Advanced **amateur** or otherwise, semi-professional, is, unlike visitors, capable, hard to detect and often with a special desire to do harm. For many in this category the main purpose is to see how much can destroy. Generally they use programming mistakes operating system to bypass authentication mechanisms and get unauthorized access to the system.

- The **professional** is different from all other types of intruders: a person well-trained, professional computer spy. These people are very good to get into a computer system (server, PC, router, etc.) and leave it without being noticed in any way. They alter or bypass logging applications of activities as easy as it may compromise any part of the system. The best defense against this attack is to avoid binding the network of systems that contain important information and strict control of physical access to them.

# Classification of risks and incidents in cyberworld

Classifications can be made according to several criteria. We will review some of them:

## Classification as a list of terms

A popular but simplistic classification is a list of defined terms. An example is as follows:

- Cables and signals interception (*Wiretapping, Eavesdropping on Emanations*);
- Searching deleted files (*Dumpster diving*);
- Denial of service;
- Harassment;
- Masquerading;
- Software piracy;
- Unauthorized copying of data;
- Degradation of service;
- Traffic analysis;
- HTrap doors;
- Covert channels;
- Viruses and worms;
- Session hijacking;
- Timing attacks;
- Tunneling;
- Trojan horses;
- IP spoofing;
- Logic bombs;
- Data diddling;
- Salamis;
- Password sniffing;
- Excess privileges;

- Scanning.

Lists of terms generally do not meet the six characteristics of a satisfactory classification.

First, the terms tend to be mutually exclusive. For example, the terms virus and logic bomb is generally found in these lists, but a virus may contain a logical bomb, so the categories overlap.

Real attackers are also using several methods. As a result, developing a comprehensive list of attack methods do not provide a good classification scheme.

## List of categories

A variation in a single list of definitions of terms is a list of categories. There is a division into seven categories:

- *Theft of passwords* - ways to get passwords from other users;
- *Social engineering* - convince people to disclose confidential information;
- *Programming errors and loopholes allowed special programs* - obtaining benefits from systems that do not meet specifications or replacement of compromised software versions;
- *Defects of authentication* - defeat mechanisms used for authentication;
- *Defects protocols* - protocols are improperly designed or implemented;
- *Leak* - use the DNS system to obtain information necessary and proper functioning of the network administrators, but can be used by attackers;
- *Denial of service* - trying to stop users to use their systems.

## Categories of results

Another variation of a list of terms is to group all the attacks in basic categories that describe the results. An example is the alteration, the flow of information and denial of service, where alteration is unauthorized modification of information, leakage is when information reaches the wrong places, and denial of service are unavailability of use networks and computers.

It is also used similar categories, but opposites in terms:

- discretion and confidentiality;
- accuracy, integrity and authenticity;

- availability.

Except intruders that will only increase access to a computer or network, or intruders using computer or network resources without degrading the service of others (theft of resources), individual attacks can be uniquely associated with one of these categories. But placing all attacks and incidents in a few categories is a classification that provides information and limited understanding.

### Empirical lists

A variation of categories of theoretical results (a priori) is developing a long list of categories based on a classification of empirical data.

- Stealing external (monitor watching over the shoulder of another person);
- External abuse of resources (destruction of a hard disk);
- Masking (recording and subsequent playback of broadcast on a network);
- Malicious software (installing a program with destructive purposes);
- Avoiding authentication or authorization (password cracking);
- Abuse of authority (falsification of records);
- Report on purpose (intentional mismanagement);
- Abuse indirectly (using another system to create a malicious program).

Classification by action - model focuses only on the information in transit and presents four categories of attacks:

- Adjournment - a good system is destroyed or becomes unusable or unavailable;
- Interception - an unauthorized party gaining access to a good system;
- Change - an unauthorized party not only gains access, but it also changes;
- Forgery - Unauthorized some inserts counterfeit objects into the system.

## Events, attacks and incidents

Three basic security concepts are important in terms of information on the Internet: *confidentiality*, *integrity* and *availability*. The concepts related to people who use this information are *authentication*, *authorization* and *acceptance*.

When the information is read and copied by someone not authorized, the result is known as loss of *confidentiality*. For some types of information, confidentiality is a very important attribute.

Examples include data obtained from research, medical and insurance records, new product specifications and corporate investment strategies. In some places, it may be a legal obligation to protect the privacy of individuals. This is true for banks and credit card companies, hospitals, medical offices, medical testing laboratories, psychological offices and agencies that collect taxes.

The information may be impaired when it is available on the insecure network. When information is changed in unexpected ways, the result is known as loss of *integrity*. This means that data been tampered with or as a result of human error or by deliberate modification. Integrity is particularly important for critical safety and financial data used in activities like electronic funds transfers, air traffic control and financial accounting.

Information can be deleted or become inaccessible, resulting in a lack of *availability*. This means that people who are allowed access to information cannot get what they want.

Availability is often the most important attribute in service-oriented businesses that depend on information (airline schedules and online inventory systems). Network availability is important for any person whose business or education depends on a network connection. When a user cannot access the network or a specific service provided by the network, it experiences a denial of service.

# Online security events, actions, and targets

Operation of computers and networks is composed of a series of *events*. An event is changing the state of a system or device. From information security point of view, these mood swings occur as a result of actions that are directed against targets. An example of an action is to enter a computer system. In this case, the action is *authenticate,* by the control program, the user access, under controlled identity of username and password.

We define thus:

- **event**, from the point of view of a computer or a computer network, as an action performed on the target system that is intended to change the system state;
- **action**, as a request for a user or program in order to obtain a result;
- **target**, as a logical entity of a network or computer system (user account, program or data) or a physical entity (PC network).

## Actions

- *Probe* - an access of a target in order to determine its characteristics
- *Scan* - Sequential access to a set of targets to determine which of them has a specific feature
- *Flood* - accessing a target repeatedly in order to overload it and cause flooding during the inaccessibility service, service being held exclusively with responses to all requests in avalanche from the flood sender
- *Authenticate* - presenting one's identity to a program and, if need, to check this identity, in order to get access to the target system
- *Bypass* - avoiding a process or program using an alternative method to access the target
- *Spoof* - action to forge the characteristics of a system or program to mimic another entity in the network
- *Read* - get the contents of a data medium
- *Copy* - reproduction without changing target
- *Steal* - taking possession of a target without keeping a copy in the original location
- *Modify* - change target content or characteristics
- *Delete* - removal or destruction of target capabilities

## Targets

- *Account* - the user access to a computer or on a network, that is controlled according to records containing the name of the account, password and rights in this area.
- *Process* - a running program, consisting of program instructions, data that are processed by the program
- *Data* - representation of facts, concepts or instructions in a manner suitable for communication, interpretation or processing by humans or automatic. The data may be in the form of files in a computer memory, hard disk, or it may take the form of a transit data through a transmission medium.
- *Component* - one of the parts that form a computer or a network.

- *Computer* - a device that consists of one or more associated components, including a processing unit and peripherals, and is controlled by the programs stored internally.

- *Network* - an interconnected group of computers, switching equipment and interconnecting branches.

- *Internetwork* - a network of networks.

# Attacks

Sometimes, an *event* that occurs on a computer or network is part of a series of steps to produce an unauthorized event. This event is then considered as part of an *attack*. An attack has several elements. First, it consists of several steps that the attacker makes. Among these steps we find an *action* brought by a *target* and the use of a *tool* to *exploit* a *vulnerability*. Secondly, an attack is intended to obtain an *unauthorized result*, viewed from the perspective of the user or administrator of the system in question. Finally, an attack is a series of voluntary steps that the attacker performs, so we have to distinguish an attack by a sequence of common actions.

Attacks have 5 parts which are logical steps that an attacker must make. The attacker uses a tool to exploit a vulnerability in order to obtain unauthorized result. To be successful, an attacker must find ways that can be connected simultaneously and repeatedly. The first two steps in an attack. tool and vulnerability, are used to cause an event to a computer or a network. More specifically, during a single attack, the attacker uses a tool to exploit a vulnerability that causes an action to an end. The logical end of a successful attack is an unauthorized result. If the logical end result of the previous steps is authorized, then virtually no attack took place.

The concept of *authorized* versus *unauthorized* is the key to understand what differentiates an attack from a normal event that occur.

- *Authorized* - approved by the user or administrator.

- *Unauthorized* - not approved by the user or administrator.

## Tools

The tool is a way to exploit the vulnerability of a computer or network.

The types od used tools are:

- *Physical atack* - a way to escape or destroy a computer, network components and support systems (air conditioning, electricity, etc.)

- *Information exchange* - a way to get information either from other attackers (e.g. IRC), or from people who are attacked (social engineering)

- *User command* - way to exploit a weakness by placing scripts in a program.

- *Script or program* - exploitation of vulnerabilities by executing a batch file (script) or a program.

- *Autonomous agent* - use of a program or piece of software that operate independently of the user, examples are network viruses and worms.

    - *Viruses* are small pieces of software that auto-reply or insert copies of its code in other programs when running an infected application. A different type of virus is "*worm*" that does not infect files on the disc, but is spreading with the network.

    - *Trojans* are also fragments of programs but not self-replication ability, being inserted into normal programs. When the user runs the program, unintentionally is running the code snippet of "Trojan horse", almost always with negative effects.

- *Toolkit* - a software package that contains commands, programs or independent agents that exploit the system weaknesses.

- *Distributed tools* - tools that are spread across multiple computers, which can be coordinated to conduct simultaneous attacks for the same target.

- *Data tap* - means to monitor electromagnetic radiation emanated by a computer or network using external equipment.

## Vulnerabilities

To get the results he wants, an attacker must use a computer or network vulnerability, which is defined as follows:

*Vulnerability* is a weakness of the system allowing unauthorized action. These are errors that occur in different stages of development, or the using of the system. They can therefore be classified in the following categories:

- *Design vulnerability* - an error that occurs during the first phase of life of a product, that of design, and that even a perfect subsequent implementation will not remove

- *Implementation vulnerability* - occurs due to the implementation phase of the project.

- *Configuration vulnerability* - occurs due to the errors made in configuring systems, such as using the default access codes or writable files with passwords

## Unauthorized results

The result is an unauthorized consequence of part of an event

- *Increased access* - an increase in unauthorized access to a computer or network
- *Disclosure of information* - the propagation of information to persons not authorized to have access to these information
- *Corruption of information* - unauthorized alteration of data on a computer or network
- *Denial of service* - intentional degradation or blocking of system resources
- *Theft of resources* - unauthorized use of a computer or network resources

Solutions of protection to these types of problems are not simple because often have to be treated their causes. It can achieve significant progress dealing with the greatest attention the security issues in the design, implementation of products, and in the use.

A summary classification of the types of incidents, along with the legal regulation of international cybercrime is shown below, in accordance with the study *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* made in 2002 by Rand Europe for the European Commission.

| Incidents | Regulatory Cybercrime Convention |
|---|---|
| Getting information about a possible target (probing, scanning) | ARTICLE 6 - Abuses on devices |
| Compromising the system by unauthorized code execution | ARTICLE 4 - Damage of data integrity<br>ARTICLE 5 - Damage of system integrity |
| Denial of service | ARTICLE 5 - Damage of system integrity |
| Compromising system (theft, modification, deletion) | ARTICLE 2 - Illegal access |

| | |
|---|---|
| Intrusion attempt | ARTICLE 2 - Illegal access, in conjunction with<br>ARTICLE 11 - Attempt and aiding |
| Unauthorized access to information | ARTICLE 2 - Illegal access<br>ARTICLE 3 - Illegal interception |
| Unauthorized access to data transmission | ARTICLE 3 - Illegal interception |
| Altering information | ARTICLE 4 - Damage of data integrity |
| Illegal access communication systems | ARTICLE 2 - Illegal access |

# Cybercrime laws

## The concept of "cybercrime"

Cybercrime is a phenomenon of our time, often reflected in the media. One study indicates that fear of attacks even exceeds the intensity to ordinary theft or fraud. Criminological research on crime made by computer systems is still under exploration. Even the most accomplished to date tend to change the way are seen the offenses in current systems of criminal justice.

Only a small proportion of criminal offenses related to the use of computer systems come to the attention of the criminal investigation bodies, so it is very difficult to achieve an overview of the extent and evolution of the phenomenon. If it is possible to achieve an adequate description of the types of offenses encountered, it is very difficult to present a synthesis based on the extent of losses caused by them, and the actual number of crimes committed. The number of cases of computer crime is growing. In Germany, 32.128 cases of such cases were reported in 1996, in the Netherlands in the period 1981-1992 was found 1400 cases, and in Japan between 1971 and 1995, 6671 cases. It is estimated that only 5% of their deeds come to the knowledge of the prosecution. To counter this lack of information, was used the process of surveys. The survey conducted by the Computer Crime Institute and Federal Bureau of Investigation (FBI) in 2003 indicated losses of 201,797,340 dollars for the 538 surveyed U.S. businesses and institutions.

Small number of reported offenses is attributed to several **causes**, among which:

- sophisticated technology used by perpetrators;
- lack of specific training of the officers of the prosecution;
- lack of a response plan in case of attack from the victims of these crimes, which can lead to the failure caused losses;
- reluctant to report crimes criminal investigation bodies.

In the latter case, even if the crime was seized, victims do not notify the prosecution to detect and punish the perpetrator. The reasons for this behavior are many. Among these, we mention concerns about the public image that could be affected by the publicity around the crime; desire not to bear the costs of any investigation, given the complexity of such research; not least, the lack of possibility to recover their losses, even if identifying the perpetrator.

Meanwhile, the cybercrime investigations are by their nature complex and involves the use of sophisticated equipment with high costs. Also, specialized staff training is a lengthy process and involves high costs. Such investigations are time consuming. A cybercrime

investigator in the field can work at maximum 3-4 cases per month, while a traditional investigator may settle between 40 and 50 cases in the same period of time.

For the purposes of this paper, we adopt the working **definition** given for the computer crimes by the OECD Expert Group in 1983:

*any misconduct, unethical or unauthorized behavior for an automatic treatment of data and/or data transmission*

This definition, although formulated more decades ago, proves its worth in the first place by allowing the integration of subsequent developments in the field of information technology.

During the present paper we will work with two definitions formulated by UNAF.

Thus, computer crime broadly means:

*any crime in which a computer or a computer network is the subject of an offense, or a computer or a network of computers is the instrument of carrying out a crime.*

Narrow by computer crime means:

*any offense the offender interferes without authorization, with automatic data processing processes.*

The content of the concept of cybercrime is extremely varied, being approached from different perspectives in the literature. Within the report of the **European Committee on Crime Problems**, cybercrimes are grouped in the following categories:

- offense of computer fraud;
- computer crime of forgery;
- offense of damage of data or computer programs;
- crime of computer sabotage;
- offense of unauthorized access to a computer;
- offense of unauthorized interception;
- offense of unauthorized reproduction of software protected by law;
- offense of unauthorized reproduction of a topography;
- offense of alteration without rights of data or software;

- computer intelligence crime;
- offense of unauthorized use of a computer;
- offense of unauthorized use of a computer program protected by law.

The manual of **United Nations** for crime prevention and control of computer makes the following categories of offenses:

- fraud by manipulating electronic computers;
- fraud by forging documents;
- alteration or modification of data or computer programs;
- unauthorized access to computer systems and services;
- unauthorized reproduction of computer programs protected by law.

The study "*The legal aspects of computer crime in the information society*" (COMCRIM study) conducted for the **European Commission** by Prof. Dr. Ulrich Sieber, University of Wurzburg, Germany, presented the following categories and sub-categories of computer crime:

- violations of privacy;
- economic offenses:
- penetration of systems to overcome technical difficulties of security ("hacking");
- intelligence information;
- piracy of computer programs;
- computer sabotage;
- computer fraud;
- distribution of illegal or harmful information (propaganda racist, dissemination of child pornography, etc.).
- other crimes:
- crimes against life;
- offenses related to organized crime;

- electronic warfare.

Cybercrime can be **classified** following different criteria. We will use for cybercrime classification the criterion of the role of computer systes in the offense. From this perspective, cybercrimes are classified into:

- *crimes committed using computer systems*, where computer systems are a tool to facilitate the commission of crime. These are "traditional" offenses improved by using computer systems; and

- *offenses committed through computer systems*, where computer systems, including data stored in them, are targeted crime. These offenses can only be committed through computer systems. They were subject to regulation in recent years.

We mention here another role that information systems can play in forensic investigation: the role of **media** and retrieval cues or evidence concerning how to commit a crime.

Awareness of the social danger of the crime such as computer triggered their criminalization in many states. He took as being the concept of "specific criminal information" as a reflection of the many new elements introduced into the criminal law to new forms of crime based on modern technology. Legislation in the field of cybercrime followed, since the '70s, several "waves". The first "wave" was prompted by the need to protect the right to privacy. Individual protection law to personal data processing were adopted in Sweden (1973), the USA (1974), Germany (1977), Austria, Denmark, France and Norway (1978), or more recently in Belgium, Spain, Switzerland (1992), Italy and Greece (1997). The second "wave" is linked to the repression of economic offenses, resulting legislative changes in the U.S. and Italy (1978), Australia (1979), UK (1981), and Switzerland (1994) and Spain (1995). A third set of rules is related to legislative intervention to protect intellectual property in the field of information technology in countries like U.S. (1980), Hungary (1983), Germany, France, Japan, Great Britain (1985) and Austria (1993), Romania (1996), Luxembourg (1997). The fourth "wave" of reforms for regulating the distribution of illegal or harmful information, and was strongly boosted in the late 80s the rise of the Internet. The fifth "wave" is related to changes in procedural law matters concerning criminal procedure issues raised within information technology, while the sixth "wave" of imposing limits and material security.

In this respect, **Council of Europe** has initiated a series of regulations on Cybercrime. Thus, in 1995 adopted Recommendation. R (95) 13 concerning problems of criminal procedural law connected with information technology on 23 November 2001, signed in Budapest Convention on Cybercrime. Convention aims to prevent acts directed against the confidentiality, integrity and availability of computer systems, networks and data, and fraudulent use of such systems, networks and data, by providing criminalize such conduct and encourage the adoption of measures that permit effective combating these types of crimes, to facilitate the discovery, investigation and prosecution of their both nationally

and internationally, and by providing substantive provisions necessary to ensure a fast and reliable international cooperation.

# Investigations

## Computer forensic investigations

Forensic investigation of computer systems has a number of features that differentiate it fundamentally from other types of investigations.

Forensic investigation of computer systems can be defined as:

*Using scientific and safe of insurance tightening, validation, identification, analysis, interpretation, documentation and presentation of digital evidence obtained from such sources such as computer science to facilitate the discovery of truth in criminal trials.*

A possible model of good practice in such computer forensic investigations include the following steps:

1. **Identification of incident** - recognition of an incident and determining its type. There is not indeed a criminal investigation stage but has a significant impact on the next steps.

2. **Preparation of investigation** - preparation of tools, verification of procedures, obtaining documents allowing search, etc.

3. **Formulation of strategy approach** - to formulate a strategy based on implied technology and possible consequences on involved individuals and institutions. The formulation of this strategy is to maximize the potential of obtaining relevant evidence while minimizing negative impact on the victim.

4. **Providing evidence** - isolation, insurance and maintenance of the physical and digital evidence. This includes the removal of which could distort the evidence in any way.

5. **Gathering evidence** - recording of physical environment and copying digital evidence using common and accepted practices and procedures.

6. **Examination of samples** - in-depth examination of the evidence, looking for items that are in relation to the offense under investigation. This involves locating and identifying samples and documenting each step in order to facilitate analysis.

7. **Analysis of samples** - determination of the significance of the evidence and pointing out the conclusions about the investigated crime.

8. **Presentation of evidence** - summarizing findings and presenting them in a manner intelligible to the layman. This summary should be supported by detailed technical documentation.

9. **Refund evidence** - if necessary, return to the rightful owners of the objects retained during the investigation. If applicable, determine, based on the provisions of the criminal procedural laws, confiscation of objects.

Forensic investigation of computer systems must provide a number of specific characteristics, required to ensure a high degree of accuracy of the conclusions. These characteristics are:

1. *authenticity* (proof of sources of evidence);

2. *credibility* (lack of doubt on the credibility and robustness of the evidence);

3. *completeness* (taking all available evidence and integrity);

4. *lack of interference and contamination* of the specimen as a result of the investigation or handling of samples after lifting.

Also, forensic investigation requires:

1. existence of pre-defined *procedures* for situations encountered in practice;

2. anticipate possible *criticism* of the methods used, on the grounds of authenticity, reliability, completeness and damage of evidence offered;

3. possibility of *duplication* of tests performed to give identical results;

4. anticipate problems for *admissibility* of evidence;

5. accepting that the research methods used at a time may be subject to *change* in future.

On this last point, it highlights a feature of forensic investigation of computer systems, ie changing forensic techniques in a very short time, modification given by the extremely rapid technological advancement globally manifested in computer science.

# Digital evidence

Digital evidence are that information with probative value for the prosecution and courts, that are stored, processed or transmitted through a computer system. They are defined as:

*any information of probative value that is either stored, processed or transmitted in a digital format.*

Digital samples include computer evidence, digital audio samples, digital video, produced or transmitted by mobile phones, digital fax, etc.

One of the particularities of this kind of evidence is that they apparently are not obvious, as contained in computer equipment that stores them. It requires investigation equipment and specific software to make these evidence available, tangible and usable.

Another aspect is the fact that these samples are very "fragile" in the sense that they can be changed or disappear very easily, in ways that are often out of reach of the perpetrators. Therefore, investigators should take special protective measures to collect, preserve and examine the evidence. Keeping these types of samples has become a growing concern of investigators around the world.

The need to standardize practice in this area has led to the development of standards on digital evidence. There are standards relating to digital evidence compiled by the International Organization on Computer Evidence (IOCE) and the Scientific Working Group on Digital Evidence (SWGDE).

# Digital sampling during investigations

Once arrived at the place where computer systems are subject to search, investigators will ensure access. Council of Europe Recommendation (95) 13 states that national legislation have to include in national legislation the obligation to provide access to computer systems, both from those who are responsible for and any person having knowledge of their operation. In addition to physical access, these individuals have a duty to provide information relating to system security information to allow investigators access to data stored in these systems.

Before proceeding to examine the systems, procedures should not neglect traditional forensic analysis of the searched space, such as physical sampling (fingerprints and other trace materials). It may also be relevant images on the monitor screen when entering the criminal investigation bodies. It can be preserved by photographing, filming, etc.

A first decision to make is the analysis of system at the ground or lifting it, and laboratory analysis.

In making this decision, you must consider the following issues:

- high quality of analysis in the laboratory;
- if the lifting computer system affects the activity of the suspect.

In that regard, have to take into consideration the recommendations of the International Chamber of Commerce, that states the rule avoid lifting systems of businesses if it would affect their normal activities.

The following criteria are useful in assessing the appropriateness of lifting systems:

- *Sample volume criterion.* Particularity of systems to enable storage to a large volume of information in a small physical space makes investigation requiring a great deal of time to obtain relevant evidence. Such research on a large time period can be driven more effective in the laboratory.

- *Criterion of technical difficulties.*

    - *The problem of avoiding destruction of the data during the investigation*. Systems analysis by investigators who do not have sufficient knowledge on the equipment or software used can destroy data accidentally.

    - *Problem of recovery of the system in the laboratory*. Due to a large variety of technical components of computers, for the system to function properly in the laboratory, have to waive all equipment present at the search. If partial lifting of system components, it is possible to have incompatibilities between the presence of high information system equipment and the laboratory (eg incompatibility of computer peripheral equipment - printers, etc.), or between programs on lifted system and laboratory equipment.

Once decided to lift the computer system at the scene of the search, have to be taken some measures to allow its exact reconstruction in the laboratory. First, shall be recorded the arrangement in space of the computer system equipment. This can be done either by shooting system from all angles, either by shooting video. In the process of photographing and filming, it is necessary to insist on the wiring connecting the various components of the equipment. Recording in camera or video version has relevance also to show the state they found equipment when lifting, thus preventing possible damage related complaints during its investigation.

In the lifting process of system components must be taken into account the need to preserve data integrity and identity. Any damage to the substrate on which the data will inevitably lead to their destruction. The prosecutors have to be specifically trained to protect evidence of an electronic nature.

Lifting procedure of computer systems is as following:

*Step 1: Close the system*. If the system was found closed when entering investigators should not be any reason on. It will proceed moving to other stages. If the system was found open, it must be closed in order to proceed to raise it. To close the system, you can use the following methods:

- disconnection from the power supply;

- closure according to normal procedure.

The first alternative is preferred if the investigator has no knowledge of computer. Some computers have uninterruptible power supplies (UPS). In this case, in addition to disconnection of the power supply system, the system must also be stopped. Disconnection will occur, in most cases, loss of data, but can avoid deleting relevant information such as temporary files that can be deleted in the normal process of closing the computer.

The second alternative is preferred when the computer is connected to the network, or when the investigator is assisted by a person who has knowledge about the functioning of that system, and about the procedures to be used for closing it.

*Stage 2: Labeling components*. If disassembly is required, each component of the system must be labeled before the configuration change, to raise evidence. If cables, are labeled both cable and media where it was disconnected. In case of holders who have not connected cables, it is advisable to be labeled "empty". It can be done and an outline of components, specifying the symbols used for labeling.

*Stage 3: Protection for changes*. All magnetic data storage must be protected against alteration of their content. Some types of hard disks have special contacts that perform write-protection. If diskettes, protection will be done by moving witness of allowing changes to "closed".

*Stage 4: Lifting the system*. Raising samples have to be done very carefully, avoiding any damage to components. It is advisable to pack components in the original packaging, if this can be found, or special packaging that assure their electrostatic protection. Also, all magnetic data storage media will be packed and sealed in such a way that access to them is enabled by disposing in the laboratory.

# The suspect

During the investigation, if the suspect is present, the prosecution would prevent any vicinity of him with the system. Especially if the suspect has superior training in computing, he may deliberately alter the data on his computer without investigators could seize it. Suspect's computer may contain some commands that can cause loss of data, commands that it is possible to be masked under the name of common commands of the operating system used.

If the suspect insists to assist investigators in the process of closing the computer or lifting process system components, they may ask the suspect to describe operations that it wants to run, and even write them on paper. Investigators will not follow the suspect directions, but will deliver to expert carrying out analysis of samples. They will be aware of the possible pitfalls introduced in this way by the suspect.

# Witnesses in cybercrime

The persons present at the search, or other person aware of the operation of the computer system, can give important information. Each witness should be interviewed on how the lifted systems are used. There are revealed the methods of input, sorting and storing data on the computer, and practices related to various aspects of its current use.

Where is investigating incidents of intrusions into computer systems of businesses, often the undertaking victim specialists are the most important source of information for the investigators. Thus, investigators should not use active penetration techniques in system for sampling, enjoying the support of those who administer the system.

In some special cases, the computers of other people, located in the same location, may have relevant evidence. For example, it cites relevant cases in which the documents have been found within the computers of secretaries of individuals under investigation.

# Transporting of samples in laboratory

Transporting samples must be carefully done, given their fragility. It is necessary to take precautions about protecting against physical shock, humidity, heat or especially the influence of electromagnetic waves. On this latter point should be avoided placing equipment near sources of electromagnetic radiation such as fax machines, copiers, radios, cell phones. It is advisable to measure the electromagnetic field with special tools where are stored the samples.

# Analysis of samples

Once brought into the lab, the components must be assembled to reconstruct the original system. For this there are used photographs or videotapes filmed before raising evidence respecting the original connections, and information obtained from witnesses in relation to practices of the use of the computer system.

The first step in analyzing samples of electronic nature is linked to the need to ensure their veracity. In order to prove the veracity of the evidence, it is necessary packaging and sealing them in the specific manner.

The first step in the protection of information systems against data modification must be done even during the search by taking measures to protect the physical storage media for writing.

It is recommended that forensic analysis of the contents of the disc to be done on a facsimile of the original disc, made in lab with software and devices. The process not only involves copying all the files on disk, but the entire contents of the disk, sector by sector, including temporary files, swap files, deleted files, even the information located on

damaged portions of the disc, etc. A copy of this nature is also now realized by special programs. It recommends to create two copies, one of them realizing proper analysis, the other as a backup.

Copying must be done by a reliable process. In order to have this feature, copying must:

- ensure the possibility of verification by third parties; the court or the opposing party must be able to verify the accuracy of the copy made.
- to have as result safe copies, that can not be forged.

It is recommended to be recorded the full detailed process of copying, indicating equipment, software and storage media used.

Safekeeping of samples is done by first copying the contents of the original systems, and conduct forensic investigations on a copy of it, having the same characteristics as the original.

As an additional security method, it can be performed mathematical authentication of the content of a storage medium, either hard disk or floppy disk, optical media, etc.. This process is achieving by mathematical processes of an image of storage media, ie image that can serve as a reference if integrity is challenged. Authentication is achieved by means of special software which provides a high degree of safety from 1 to several millions.

# Preparing team members

Nature of crime requires criminal investigation to achieve within a team of investigators. The need of the investigation within a team emerges from the need to ensure a greater objectivity and effective conjugation skills and specializations derived from team members. Both because of the special characteristics of the equipment subject to investigation and methods employed in the forensic investigation of information systems, team members investigators must possess adequate knowledge and skills specific to the investigation.

It is estimated that a good investigator must possess:

- sufficient knowledge of computer techniques that allow it to understand the functioning philosophy of a computer system, examine technical documentation and to use, if needed, advanced computer techniques to help him achieve the pursued aim;
- sufficient knowledge on the techniques used by companies, especially accounting systems, in order to understand the characteristics of systems that could be subject to fraud, so that it can determine both mode and where might to direct the investigation to find evidence of the offense;

- sufficient knowledge of internal security techniques so that the investigation can be carried out quickly and reliably, and be directed in the right direction.

In addition to the knowledge of the investigators, it was highlighted skills that must exist or be developed in individual investigators so that they may conduct the investigation. Thus, we can mention: extroverted personality (because generally specialists in technical fields, particularly computer, possesses fewer inter-human communication skills), inclination to detail (very important, especially given the specific of electronic evidence: abundance of information available on storage space, reduced physical size; however, it is important to keep an overall view of the investigation), logical thinking, good communication (especially important to ensure the presentation of the results of the investigation in a relevant both in writing and in court), objectivity. Preparing cybercrime investigators in the field is a constant concern of the criminal investigation bodies worldwide.

# Computer tools

Forensic investigation of computer systems requires specific tools. As equipment, the investigators must have data storage media in sufficient quantity and quality to enable copying them from the computer system under investigation.

In analyzing of computer systems, it is used a significant number of computer programs. As an example we can mention programs for the exact copy of the contents of physical memory, for analysis and comparison of files, for cataloging disc contents, for mathematics validation and authentication of data, for recovering deleted files, decrypt, or antivirus programs. It is necessary that the software used by the prosecution to be registered in terms of copyright protection belonging to the producers of these programs.

# Convention on Cybercrime

Council of Europe: Convention on Cybercrime - CETS No.: 185

## Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognizing the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalization, convergence and continuing globalization of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognizing the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions

without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighboring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

## Chapter I – Use of terms

### Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

## Chapter II – Measures to be taken at the national level

### Section 1 – Substantive criminal law

***Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems***

### Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining

computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article 3 – Illegal interception**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article 4 – Data interference**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

**Article 5 – System interference**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

**Article 6 – Misuse of devices**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

***Title 2 – Computer-related offences***

## Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

## Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

***Title 3 – Content-related offences***

## Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

***Title 4 – Offences related to infringements of copyright and related rights***

## Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and

Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

***Title 5 – Ancillary liability and sanctions***

## Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

## Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

### Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

## Section 2 – Procedural law

***Title 1 – Common provisions***

### Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

**Article 15 – Conditions and safeguards**

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

***Title 2 – Expedited preservation of stored computer data***

## Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

***Title 3 – Production order***

## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

***Title 4 – Search and seizure of stored computer data***

## Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible

from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

***Title 5 – Real-time collection of computer data***

## Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### Section 3 – Jurisdiction

### Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

## Chapter III – International co-operation

### Section 1 – General principles

***Title 1 – General principles relating to international co-operation***

### Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of

investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

***Title 2 – Principles relating to extradition***

## Article 24 – Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the

Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

***Title 3 – General principles relating to mutual assistance***

## Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

## Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in

initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

***Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements***

## Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

## Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

## Section 2 – Specific provisions

***Title 1 – Mutual assistance regarding provisional measures***

## Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

**Article 30 – Expedited disclosure of preserved traffic data**

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a

sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

***Title 2 – Mutual assistance regarding investigative powers***

### Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

### Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

### Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

### Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

***Title 3 – 24/7 Network***

### Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

## Chapter IV – Final provisions

### Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

### Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into

force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

**Article 39 – Effects of the Convention**

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

**Article 40 – Declarations**

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

**Article 41 – Federal clause**

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between

its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

**Article 42 – Reservations**

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

**Article 43 – Status and withdrawal of reservations**

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

**Article 44 – Amendments**

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration

of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

**Article 45 – Settlement of disputes**

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

**Article 46 – Consultations of the Parties**

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend

the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

**Article 47 – Denunciation**

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

**Article 48 – Notification**

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which

have participated in the elaboration of this Convention, and to any State invited to accede to it.

# Recommendation No. R (95) 13

COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (95) 13

**OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURAL LAW CONNECTED WITH INFORMATION TECHNOLOGY**

*(Adopted by the Committee of Ministers on 11 September 1995, at the 543rd meeting of the Ministers' Deputies)*

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Having regard to the unprecedented development of information technology and its application in all sectors of modern society;

Realising that the development of electronic information systems will speed up the transformation of traditional society into an information society by creating a new space for all types of communications and relations;

Aware of the impact of information technology on the manner in which society is organised and on how individuals communicate and interrelate;

Conscious that an increasing part of economic and social relations will take place through or by use of electronic information systems;

Concerned at the risk that electronic information systems and electronic information may also be used for committing criminal offences;

Considering that evidence of criminal offences may be stored and transferred by these systems;

Noting that criminal procedural laws of member states often do not yet provide for appropriate powers to search and collect evidence in these systems in the course of criminal investigations;

Recalling that the lack of appropriate special powers may impair investigating authorities in the proper fulfilment of their tasks in the face of the ongoing development of information technology;

Recognising the need to adapt the legitimate tools which investigating authorities are afforded under criminal procedural laws to the specific nature of investigations in electronic information systems;

Concerned by the potential risk that member states may not be able to render mutual legal assistance in an appropriate way when requested to collect electronic evidence within their territory from electronic information systems;

Convinced of the necessity of strengthening international co-operation and achieving a greater compatibility of criminal procedural laws in this field;

Recalling Recommendation No. R (81) 20 on the harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers, Recommendation No. R (85) 10 on letters rogatory for the interception of telecommunications, Recommendation No. R (87) 15 regulating the use of personal data in the police sector and Recommendation No. R (89) 9 on computer-related crime,

Recommends the governments of member states:

i. when reviewing their internal legislation and practice, to be guided by the principles appended to this recommendation; and

ii to ensure publicity for these principles among those investigating authorities and other professional bodies, in particular in the field of information technology, which may have an interest in their application.

# Appendix to Recommendation No. R (95) 13

***concerning problems of criminal procedural law connected with information technology***

## I. Search and seizure

1. The legal distinction between searching computer systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied.

2. Criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein.

3. During the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction which are connected by means of a network and to seize the data therein, provided that immediate action is required.

4. Where automatically processed data is functionally equivalent to a traditional document, provisions in the criminal procedural law relating to search and seizure of documents should apply equally to it.

## II. Technical surveillance

5. In view of the convergence of information technology and telecommunications, laws pertaining to technical surveillance for the purposes of criminal investigations, such as interception of telecommunications, should be reviewed and amended, where necessary, to ensure their applicability.

6. The law should permit investigating authorities to avail themselves of all necessary technical measures that enable the collection of traffic data in the investigation of crimes.

7. When collected in the course of a criminal investigation and in particular when obtained by means of intercepting telecommunications, data which is the object of legal protection and processed by a computer system should be secured in an appropriate manner.

8. Criminal procedural laws should be reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offences against the confidentiality, integrity and availability of telecommunication or computer systems.

## III. Obligations to co-operate with the investigating authorities

9. Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority.

10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedural law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.

11. Specific obligations should be imposed on operators of public and private networks that offer telecommunication services to the public to avail themselves of all necessary technical

measures that enable the interception of telecommunications by the investigating authorities.

12. Specific obligations should be imposed on service-providers who offer telecommunication services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authority.

## IV. Electronic evidence

13. The common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognised. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to traditional documents should similarly apply to data stored in a computer system.

## V. Use of encryption

14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.

## VI. Research, statistics and training

15 The risks involved in the development and application of information technology with regard to the commission of criminal offences should be assessed continuously. In order to enable the competent authorities to keep abreast of new phenomena in the field of computer-related offences and to develop appropriate counter-measures, the collection and analysis of data on these offences, including *modus operandi* and technical aspects, should be furthered.

16. The establishment of specialised units for the investigation of offences, the combating of which requires special expertise in information technology, should be considered. Training programmes enabling criminal justice personnel to avail themselves of expertise in this field should be furthered.

## VII. International co-operation

17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established.

Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

18. Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorised to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorised to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented.

# Rules for obtaining digital evidence by police officers

(Source: Australasian Centre for Policing Research)

- OFFICER SAFETY COMES FIRST!
- Search any visible or broken cable. If you have doubts about the safety of handling, ask an expert.
- Make sure you have the right to frisk and lift the evidence.
- DO NOT use the keyboard or mouse.
- DO NOT attempt to examine the contents of the computer, you could alter evidence.
- Record all actions for lifting samples.
- If the computer system is closed, DO NOT open.
- If the computer system is open, shoot the screen before going further.
- DO NOT close the computer system in the normal manner. Remove the power cord from the computer directly, not from the socket. Make sure you do this safely.
- Do not ignore other types of evidence such as fingerprints on the equipment.

# Standards in the field of digital forensics

(Source: Scientific Working Group on Digital Evidence)

**Principle 1**

In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

**Standards and Criteria 1.1** All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

**Standards and Criteria 1.2** Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

**Standards and Criteria 1.3** Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.

**Standards and Criteria 1.4** The agency must maintain written copies of appropriate technical procedures.

**Standards and Criteria 1.5** The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure.

**Standards and Criteria 1.6** All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

**Standards and Criteria 1.7** Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

# Principles in digital evidence

(Source: International Organization on Computer Evidence)

1. In the process of obtaining digital evidence, actions taken should not alter the evidence.

2. Where it is necessary for a person to access original digital evidence, that person must be competent in terms of crime.

3. All activities related to the investigation, storage, examination or transfer of digital evidence must be fully recorded in writing, kept and available for evaluation.

4. A person is responsible for all activities related to digital evidence as long as they are in his possession.

5. Any organization responsible for investigating, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

# Procedures model for the forensic examination

(Source: International Association of Computer Investigation Specialists)

## Hard disk examination

- Sterile conditions are established in terms of crime. All storage media used during the examination are prepared recently, cleaned of extraneous data, anti-virus checked and tested before use;
- All used software licensed and can be used by the institution;
- The original computer is physically examined. It is provided a description of the hardware that is registered. Comment any unusual item encountered during the physical examination of the computer system.
- All precautions are taken during copying or access to the original storage media in order to prevent the transfer of viruses, destructive or other inaccuracies in the content / the original storage media. It is recognized that due to hardware limitations and operating systems this is not always possible;
- CMOS contents and internal clock are checked and data accuracy and time is recorded. Date and time clock is frequently important for setting the date and time of file creation or modification.
- Normally, the original storage media are not used in the investigation. An identical copy or a true original storage environment will be achieved. This copy or image will be used for the actual examination. There will be recorded a detailed description of the creation of the copy or image.
- Copy or image of the original hard drive will be examinate and a description of what was seen have to be registered.
- Boot data and operational command files and system configuration, user defined (such as CONFIG. SYS or AUTOEXEC.BAT) are reviewed and a description of what was seen have to be registered.
- All deleted files that can be recovered will be saved. Where useful or possible, first character of recovered files will be changed from HEX E5 in "-" or otherwise unique character for identification purposes.
- It performs normally, a listing of all the files contained in the media examined, whether or not they contain potential evidence.

- Where appropriate, the unallocated space is examined to identify hidden or lost data.
- If applicable, the idle space corresponding to each file is examined to identify hidden or lost data.
- Examine the contents of each data file from the roor directories and each sub-folder (if applicable).
- Password protected files are unlocked and examined.
- Make a print or a copy of everything seemingly constitute evidence. The file or location where any such evidence was obtained is denoted on each printed sheet. All samples are labeled, numbered in order and properly insured and forwarded.
- Executable programs of specific interest will be considered. User data files that could not be accessed by other means will be examined using the default application.
- Comments and conclusions will be documented properly.

# Code of Ethics

(Source: International Association of Computer Investigation Specialists)

1. Maintain the highest level of objectivity in all forensic investigations and present the facts correctly;
2. Examine and analyze in detail the evidence;
3. Examine in compliance with established principles and validated by practice;
4. Issue opinions based on facts that can be reasonably demonstrated;
5. Do not hide any fact likely to remove offending or criminal liability, that might distort the elements of an investigation;
6. Do not misrepresent your education, experience and membership in professional organizations;
7. Help and advise any investigator, regardless of the institution he work for.

# Sources and references

Ministry of Communications and Information Technology, Romania

Achim, Gheorghe, *Metodologia investigării criminalistice a fraudelor informatice*, Editura Omnia, 2000

Amza, Tudor, Amza, Cosmin-Petronel, *Criminalitatea informatică*, Ed. Lumina Lex, 2003

Antoniu, George, *Infracţiuni în legătură cu folosirea calculatoarelor*, în Studii de Drept Românesc, 3/1992, p. 227-243.

Antoniu, George, *Les crimes informatiques et autre crimes dans le domaine de ela technologie informatique en Roumanie*, în Ius Informationis vol. 6, 1994, p. 409-419.

Antoniu, George, *Vinovăţia penală*, Ed. Academiei Române, Bucureşti, 1995.

Antoniu, George, Bulai, Constantin (coord.), *Practica Judiciară Penală*, Ed. Academiei Române, Bucureşti, 1998, vol. V, Infracţiuni prevăzute în legi speciale.

Association of Chief Police Officers, *Good Practice Guide for Computer based Electronic Evidence*, 2003.

Banks, Michael, *PC Confidential*, Ed. All, 2001

Bates, Jim, *Fundamentals of Computer Forensics*, în International Journal of Forensic Computing, ian/feb 1997

Berryhill, Jon, Berryhill, Katie, *Computer Forensics*, în Police and Security News, sept. 1997

Bica, Gheorghe, Mihail, Gheorghe, *Infracţiuni săvârşite prin calculator*, în Revista de Drept Penal 4/1996, p. 85-88.

Bulai, Costică, *Manual de Drept Penal*, Ed. All, Bucureşti, 1997.

Casey, Eoghan (ed.), *Digital Evidence and Computer Crime: Forensic Science*, Computers, and the Internet, Academic Press, 2004

Centrul de Expertiză şi Răspuns pentru Incidente de Securitate

Dierks, Michael P., *Computer Network Abuse*, în Harvard Journal of Law and Technology, spring 1993, p. 307-342 (6 Harv. J. L. & Tech. 307)

E-frauda

Translated and adapted by Nicolae Sfetcu

The texts from this book are under a Creative Commons Attribution-ShareAlike License.

# About

## Nicolae Sfetcu

Owner and manager with MultiMedia SRL and MultiMedia Publishing House.

Project Coordinator for European Teleworking Development Romania (ETD)

Member of Rotary Club Bucuresti Atheneum

Cofounder and ex-president of the Mehedinti Branch of Romanian Association for Electronic Industry and Software

Initiator, cofounder and president of Romanian Association for Telework and Teleactivities

Member of Internet Society

Initiator, cofounder and ex-president of Romanian Teleworking Society

Cofounder and ex-president of the Mehedinti Branch of the General Association of Engineers in Romania

Physicist engineer - Bachelor of Physics, Major Nuclear Physics. Master of Philosophy.

### Contact

Email: nicolae@sfetcu.com

Facebook/Messenger: https://www.facebook.com/nicolae.sfetcu
Twitter: http://twitter.com/nicolae
LinkedIn: http://www.linkedin.com/in/nicolaesfetcu
YouTube: https://www.youtube.com/c/NicolaeSfetcu

# Publishing House

## MultiMedia Publishing

*web design, e-commerce and other web applications * internet marketing, SEO, online advertising, branding * software localization, English - Romanian - French translation * articles, desktop publishing, secretarial services * powerpoint, word and pdf presentation, image, audio and video editing * book and e-book conversion, editing and publishing , isbn*

Email: office@multimedia.com.ro

MultiMedia: http://www.multimedia.com.ro/
Online Media: https://www.telework.ro/

Facebook: https://www.facebook.com/multimedia.srl/
Twitter: http://twitter.com/multimedia
LinkedIn: https://www.linkedin.com/company/multimedia-srl/